Volume : 4 | Issue : 5 | May 2015 • ISSN No 2277 - 8179

Edging Trust in Cloud Enviroment

Engineering

KEYWORDS : Cloud, Trust Audit, Transparency,SLA-Service Level Aggreement, Information Security

Affreen Ara MTech ,Padmanava College of Engineering ,Rourkela, India

ABSTRACT

Cloud Computing is an internet based computing system ,which allows users to share resources, information, software and services through a distributed network. This paper describes about trust in cloud environment. In this paper we present some measures in relation to security and prevention. The methodology of my study is from secondary resources such as journals, articles, papers, blogs and conference proceedings. There are many standards for cloud environment which needs to be implemented by every data provider .In present scenario, there has been a growing concern about security with multitude of security breaches last year and to build trust there is an urgent need to address these issues. Topics covered in this paper include the terms ,characteristics, architecture ,deployment types of Cloud Computing, .It discuses about concept of Trust ,Trust level in cloud ,Information Security, Cloud Audit in an enterprise cloud environment.

INTRODUCTION

With the advent of internet business have moved to whole new avenue that is cloud. In the year 2009 there were 2.5 billion devices connected to the internet .These devices were PC, laptop, smart phone, I pad, wearable devices, and smart watches. By the year 2020 there will be rapid increase in number of users totaling up to 30 billion .In present age trust is critical ;open standards are standard foundation of which internet technology was constructed .Web applications are rich with content, risk in organization increases, brand and data have become most costlier as ever. In today's competitive world brand image is associated with trust and suffers if trust is breached in any way. As trust takes years to build but it takes a minute to lose it. Every day there are new reports of highly collaborated cyber attacks on a reputed websites. The total number of security breaches made in the year 2013 count to almost 619 according to Identity Theft Resource Centre. There is a sincere need to analyze and find solution to prevent such future attacks.

CLOUD COMPUTING

The Cloud computing term has come from the word that describes what happens when applications and services are moved to the internet. The Cloud computing is a distributed network that uses large number of computers connected to real time communication over the internet. In present day there are many companies that offer cloud services like Enomaly, Google ,Microsoft, Yahoo, NetSuite, Eucalyptus, Rackspace, Amazon ,AT & T, GoGrid ,Salesforce.com and many more.The National Institute for Standards and Technology (NIST), Information Technology Laboratory offers this definition of Cloud Computing[64] as follows.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Essential Characteristics

Cloud computing has following characteristics [8]:-

Shared resources pooling: It uses virtualization technique which enables sharing of resources like memory, physical services and network resources by the users.

Metered service: The subscription based companies' bill customers for cloud service according to their actual use during the billing period.

Dynamic provisioning: It allows prerequisite of resources based on real time demand. The user need not worry about maintenance and set up

Broad networked access: It needs to be accessed through internet network.

Service based: Cloud offers three types of service which are Infrastructure as Service, Platform as Service and Software as Service.

Architectural lavers of cloud

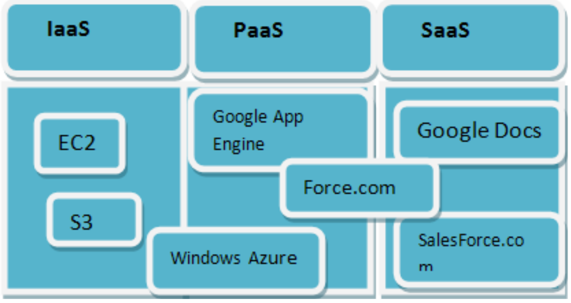


Figure-1 Architecture layers of cloud

There are three types of service models

Cloud Software as a Service (SaaS): It is also called as Service[13] or Application Cloud. It is a type of service where applications are delivered on cloud, are provided to the users based on subscription and on demand basis.eg Microsoft Web Apps of Microsoft, Google and SalesForce.com.

Cloud Infrastructure as a Service (IaaS):It is also called as Resource Cloud. It provides the user, the capability to control and manage in terms of operating system , application ,storage and network connectivity to enhance virtualization options on pay as you use basis. But the user does not control the cloud structure.

Cloud Platform as a Service (SaaS):It provides computational platform for users to deploy applications onto cloud infrastructure which are either consumer created or acquired application developed by API provided by cloud service provider. eg Windows Azure, Google App Engine etc.

Deploying cloud services depends on many requirements. Deployment types

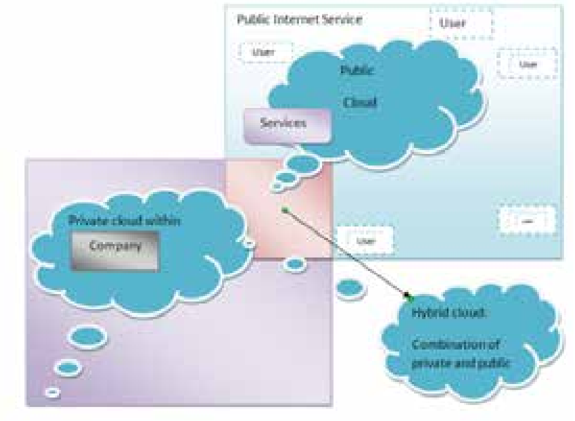


Figure 2-Cloud Deployment types

Public Cloud: The cloud infrastructure which is available to general public or large community by a service provider .It provides the end user the capability to exploit cloud features for her/his own benefit.eg Google App., Amazon, Window Azure.

Community Cloud: The cloud infrastructure which is shared by more than one organization also share common goals and interests.

Private Cloud: These are solely owned by respective organizations .This type of cloud is managed by an organization itself or third party service provider. eg Amazon

Hybrid Cloud: Hybrid cloud is the amalgamation of two or more clouds (public, community or private). They have the ability to move data and applications from one cloud to another.

TRUST

Trust means act of faith, confidence and reliance in something that is expected to deliver or behave as promised. Trust can also be stated *as level of confidence in something or on someone* .Hence we can also say that trust is customer's level of confidence or faith in using cloud services. Trust is a wider[38] notion than security it includes subjective criteria and experience. There exists both hard and soft trust. Hard trust involves entities like authenticity, encryption and security in transaction whereas soft trust involves entities like human psychology, brand reliability and user friendliness.

Choosing the right service provider

There are many service[29] providers each offering different type of service. Sometimes Enterprise tries to use more than one service provider placing different workload to different provider. This builds up problems with different parameters of billing schemes and service agreements. Choose a provider who is flexible to work with load under multiple environments. Service provider must give good performance, security and resiliency. The customer should read and ask questions before signing the service agreement. The enterprise should select such a provider that makes physical security of cloud as high priority. The provider should ensure measures to segregate enterprise workload on physical servers, securing firewall for optimal protection against internet attackers, data encryption and define administrative access controls. When an enterprise entrust its information to a service provider, its responsibility is to protect the customer assets.

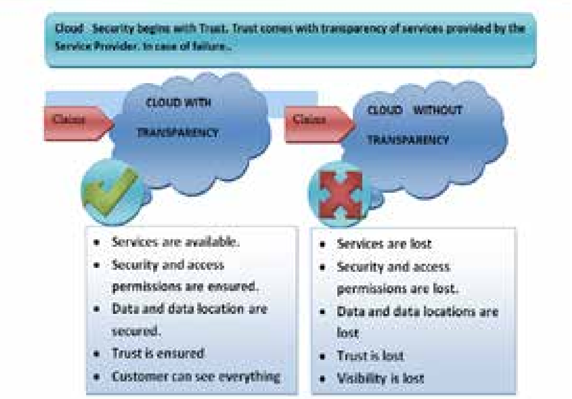
Trust level in SLA

With growing number of enterprises willing to adopt cloud services specialist feel that cloud is slowly winning trust . The service provider[51] needs to offer Service Provider Agreement (SLA) to gain trust of customer. If a cloud provider cannot invest money in architecture it is possible that he may not be able to keep terms of SLA. If the service provider fails to meet keep up the agreement he may end up paying more money to the customer. The service provider should carry out realistic assessment of their scientific capabilities, as well of their budget to prevent SLA violations. It is important for cloud providers to incorporate SLA to ensure trust and transparency in cloud services. There is a need of serious thinking about how safeguarding trust; in potential risk of vulnerabilities both identified and unknown ones .The vendors should do as much as necessary to protect its users.

The customer [41] need to know whether there has been breach in cloud service. As large enterprises are relying more on cloud services, they should sign SLA agreement that includes a clause regarding alerting customers and response in case there is a security failure in cloud. Maintaining a positive communication with customers is essential for building trust in cloud. The provider must keep the customer updated about development after disruption of cloud services by which he can acquire the confidence of the customer.

Transparency

A trusted[38] cloud is a cloud that harmonizes the security for the transaction with comprehensive transparency of control and result such that it conveys evidence based confidence with system within its environment operates as advertised , and that no unadvertised function are occurring.



Cloud : Security begins with Trust. Trust comes with transparency of services provided by the Service Provider. In case of failure..

- Services are available.
- Security and access permissions are ensured.
- Data and data location are secured.
- Trust is ensured
- Customer can see everything

- Services are lost
- Security and access permissions are lost.
- Data and data locations are lost
- Trust is lost
- Visibility is lost

Figure: Transparency in cloud can be achieved by using Transparency as a service(TaaS)

International Standard Organization ISO 27001 and ISO 27002 are foundation standards for IT environment to build transparent security system and enabling assurance though use of structured governance and security framework .Cloud Trust Protocol is an important component of Cloud Security Alliance's Security, Trust & Assurance Registry STAR(CSA STAR)which aims to deliver Transparency as a Service. Transparency helps in building trust with the customers. Once transparency is lost then security, value and compliance is lost as well. Vendors should inform their customers about their-

- Cloud vendors must be clear about their Service agreement signed with the customers.
- Infrastructure provided: Customers should have clear knowledge, understanding of service and infrastructure provided about the vendors.
- Disaster Recovery Plan: Vendors should update customer about disaster recovery procedures in case of service failure.

Security Controls

Implementing security controls in cloud is one of the most critical elements for trust .Providers need to focus on data centric approach towards security. The European [52] Union Cyber Security Agency investigated how the process of disaster reporting would be set up. The executive director of European Agency for Network and Information Security ENSIA Professor Udo Helmbrecht noted that "*Incident reporting is crucial to enable better understanding of the security and resilience of Europe's critical information infrastructures. Cloud computing is now becoming the backbone of our digital society, so it is important that cloud providers improve transparency and trust by adopting efficient incident reporting schemes.* "

With rapid risk in security cloud providers will need to collaborate with third party security providers to produce better security solution for future. Microsoft decided to end support for Microsoft XP in the year 2013, but it is still used in corporations, hospitals, government, colleges and by individuals. Systems such as Windows XP are in high risk of being infected compared to its other versions. So organizations need to update their operating system to avoid security risks. Providers and consumers need to make a combined effort to preserve trust and build a healthy relationship in cloud environment.

INFORMATION SECURITY

Service providers need to assure customer about security provisions which are provided to the user; it is the key to establish trust. Trust is one of the main constraints in online cloud environment because consumers need to share huge amount of private data to the data provider. The users face the dilemma of disclosing their personal information and information used to store and create business profiles. The surveillance program by the National Security Agency in the year 2013 has ignited concerns about vulnerability of data store in cloud .Gmail decided to encrypt its email system using HTTPS connection. The HTTPS protocol ensures that mail cannot be traced as it travels from the computer to Google data server .The message inside the Google server is encrypted and protected too. The Information Technology and Innovation Foundation said that these leaks could cause US providers to close 10-20% foreign market overseas competitors up to 35$ billion potential sales through 2014. These leaks indicate that how little control the companies have over data. There is urgent need to address security issues of data encryption, key encryption, identity theft, data integrity, and availability, and confidentiality, access control, cross VM attacks, data ownership and regionalization for government transparency to improve security. Today major data providers such as Yahoo, Microsoft and Google are using encryption methods such as 128 bit AES for securing data . Cipher Cloud is an advanced cloud security technology that uses AES 256 bit encryption. AES is a symmetric key algorithm which uses same key for encryption and decryption.SSL patented technology provides secure virtual indexing at gateway while sending encrypted data to cloud which is certified by NIST.

AUDITS

Audit is a plan for presentation of information about how the service provider addresses the control framework. It also reduces cost, deployment risks, as well as alleviates problem of selecting a service provider. Most of the organizations are experienced in traditional deployment methods such as auditing and assessment but with rapid use of evolving cloud technologies these activities become more complicated. Physical controls are needed to protect physical data which is stored in disk drives in data centers. Cloud providers are hesitant to endorse testing procedures in shared environment. When an organization moves into cloud it does not know how to assess threat or choose a service provider that can alleviate risk. Auditing is extremely critical for present day cloud users and service providers.

The cloud development framework[20] is known as A6(Automate Audit, Assessment Assurance and Assertion). According to CSA (Cloud Security Alliance);

Cloud Audit is to provide a common interface and namespace that allows interested enterprises and service providers to automate the Audit, Assertion ,Assessment and Assurance of their infrastructure such as Service as a Infrastructure, Platform as a Infrastructure and application Software as a Infrastructure by using an open extensible and secure methodology. It utilizes security automation capabilities with existing protocols via a standard open extensible set of interface that offers primitive definition and language structure using Hypertext Transfer Protocol. It also allows for the extension and elaboration for the service provider and choice of trusted assertion validation sources and checklist definitions.

Objective of Auditing:

- It provides user a balanced evaluation of accessibility to rely on data provider
- It finds the depth and efficiency of the data provider internal system and measurement.
- It allows finding out what quality of the service is provided to user in comparisons to other providers.
- It discovers issues in organization capability to crossing point with other service provider and provides uninterrupted service.

The cloud service provider and customers need to collaborate between themselves to perform audits. The service provider should document events, physical risks, configurations to meet the customer requirements. The user needs to maintain application installed logs; operating system logs files and local surveillance data. Audit information is provided by three sources the cloud service provider, customer and third party. The data provider should make a point to submit audit reports such as SAS-70, Service Organization Control-SOC-1,SOC-2 and SOC-3 to the customer .As trust come by maintaining good relationship with customers in addition to it needs a good track record too.

CONCLUSION

Cloud computing goes beyond boundaries, technology is growing enormously; there is rapid growth in use of mobile devices, service provider need to develop good security strategies to enable secure business with customer. Today more people are using mobile application; there comes a demand for qualified security expert to understand mobile vulnerabilities. There is a dire need to understand and explore vulnerabilities in web and internet with rise of emerging threat intelligence . Service providers need to follow security controls and proper standards to ensure trust of it users. They is need to maintain transparency with users regarding their policies and ensure an effective management system. Trust comes with good reputation, the goal is to improve business and have a competitive edge in today's market. The cost of defending against cyber attack remain high ,but gaining visibility into threats and mitigating risk can help a lot in future.

REFERENCE

[1] Keith Jeffery , and Burkhard Neidecker-Lutz ," The future of Cloud Computing, Opportunities for European cloud computing beyond "2010 . Expert Group Report Public Version 1.0 for European Commission Information Society and media. | [2] Neil Readshaw,.Martin Borrett,"How does IBM deliver cloud security ", An IBM paper covering SmartCloud Services. | [3] David Lingenfelter" Cloud Audit and Cloud Trust Protocol " © 2011 Fiberlink Communications, | [4] Danan Thilaknathan, Shiping Chen, Surya Nepal ,Rafale A Calvo" Secure data Sharing in cloud," DOI: 10.1007/978-3-642-38586-5_2, © Springer-Verlag Berlin Heidelberg 2014. | [5] Farhan Bashir Shaikh and Sajjad Haider ,"Security Threats in Cloud Computing", IEEE , at 6th international conference on internet technology and secure transactions 11-14 Dec 2011 Abu Dhabi UAE. | [7]Frost ansd Sullivian, "Tips for choosing right service provider", an Executive summary provided by IBM. | [8] Kapil Bakshi," Cisco Cloud Computing" ,Data center strategy, Architecture and Solutions ,point of view white paper for us public sector 1st edition. | [9]" Audit and Assurance ", published by the National IT and Telecom Agency march 2011 . | [10]Alex Huth and James Cebula, "The basics of Cloud Computing". | [11] Nick Coleman, and Martin Borrett, "Cloud Security who do you trust ?" by IBM. | [12] Qi Zhang , • Raouf Boutaba ,Lu Cheng, " Cloud computing: state-of-the-art and research challenges", Published online: 20 April 2010 © The Brazilian Computer Society 2010. | [13]"Security guidance for critical areas of focus in cloud computing v3.0" by Cloud Security Alliance. | [14] Khaled M. Khan and Qutaibah Malluhi ,"Establishing Trust in Cloud Computing", Qatar University. | [15] Siani Pearson ,"Privacy, Security and Trust in Cloud Computing " by HP Laboratories HPL-2012-80R1. | [16] Cong Wang , Wenjing Lou and Kui Ren," Toward Publicly Auditable Secure Cloud Data Storage Services Cloud computing ", Illinois Institute of Technology. | [18] Ron Knode ,"CloudTrust 2.0 In the Cloud, „Security""Starts with a T"" Lubricating digital trust in the cloud with SCAP 28 September 2010 . | [19] Lee Badger, David Bernstein, Robert Bohn, Frederic de Vaulx, Mike Hogan, Jian Mao, John Messina, Kevin Mills, Annie Sokol, Jin Tong, Fred Whiteside and Dawn Leaf NIST national Institute of Satndards and technology . | [20] Frank Simorjay, Ariel Silverstone , Aaron Weller The Microsoft approach to cloud transparency Using the Cloud Security Alliance's Security, Trust & Assurance Registry (STAR). | [21] Jeff Frazier, "Trust Clouds An Emerging, Horizontal Information-sharing Service for Governments " , Cisco Internet Business Solutions Group ,January 2009. | [22]" EMERGING CYBER THREATS REPORT 2014" Presented by the Georgia Tech Information Security Center (GTISC and the Georgia Tech Research Institute (GTRI) Georgia Tech Cyber Security Summit 2013. | [23] Ali Khajeh-Hosseini , Ilango Sriram Ian Sommerville ",Research Challenges for Enterprise Cloud Cloud Computing", Co-laboratory School of Computer Science University of St Andrews UK Department of Computer Science. | [24] Ryan K L Ko 1, Peter Jagadpramana 1, Miranda Mowbray 2, | Siani Pearson 2,Markus Kirchberg 1, Qianhui Liang 1, Bu Sung Lee; | TrustCloud: A Framework for Accountability and Trust in Cloud | Computing". | [25] "Creating Trust in the Cloud", Intel and Canonical | [26] Jogesh K Muppala1*, Deepak Shukla1, Subrota K Mondal1 and Pranit Patil2,;"Establishing Trust in Public Clouds," Hong Kong University of | Science & Technology | [27] Mr. Deepak Singh Chouhan , "Building Trust In Cloud Using | Public Key Infrastructure A step towards cloud trust" IES IPS Academy Indore | India (IJACSA) International Journal of Advanced Computer | Science and Applications, Vol. 3, No. 3, 2012. | [28] Roland A. Burger, christian cachin, Elmar Husmann, "Cloud, Trust, | Privacy Trustworthy cloud computing whitepaper". | [29]" White Paper Cloud Computing.Alternative sourcing strategy for | business ICT " Published by:T-Systems Enterprise Services Germ.any. | [30] "Cenzic Application Vulnerability Trends Report : 2014" | [31]" Trend micro blurring boundaries trend micro security predictions | for 2014 and beyond " . | [32] "HP Mobile Application Security Vulnerability Report – NOV 2013 ". | [33] "BUILDING CUSTOMER TRUST IN CLOUD COMPUTING | WITH TRANSPARENT SECURITY White Paper" by Sun Microsystems | November 2009. | [34]"Security Threat Report 2014 Smarter, Shadier, Stealthier Malware" by Sophos. | [35]" Protecting your brand in the cloud Transparency and trust through enhanced | reporting" November 2011. | [36] Willaim Jackson, " An emerging target for cyber attacks Trust – GCN" on jan | 2013 http://gcn.com/blogs/cybereye/2013/01/trust-infrastructure-top-cyber- | targets.aspx. | [37]David Baker , " Building Trust and Security Through Transparency of | ServiceCloud Security Alliance Blog ", https://blog.cloudsecurityalliance.org/2013 | /05/21/building | -trust-and-security-through-transparency-of-service/. | [38]Ronald B Knode,Digital Trust in Cloud Liquid Security in cloudy places,Aug 09 | | [39]Warwick Ashford,"Security in the cloud Top nine issues in building users' trust " | ,http://www.computerweekly.com/feature/Security-in-the-cloud-Top-nine-issues-in- | building-users-trust. | [40]Seth Payne,"Building trust between cloud providers and consumers - Network | World" http://www.networkworld.com/news/tech/2013/030413-cloud-providers-26 | 7301.html. | [41] "Building trust in the cloud - EY – Global" http://www.ey.com/GL/en/Services/ | | Advisory/Building-trust-in-the-cloud | [42] Spearcy,"Business Continuity and Disaster Recovery Planning for the Cloud". | In year 2013 ; http://www.datavail.com/category-blog/business-continuity-planning- | disaster-recovery-in-the-cloud/. | [43] Sabi Goriawala," Can You Trust The Public Cloud @VMblogcom ",. | http://vmblog .com/archive/2014/04/07/can-you-trust-the-public-cloud.aspx | [44]Matt Prigge, "Cloud audits often don't mean what you think they do Data | Explosion – InfoWorld ",http://www.infoworld.com/d/data-explosion.html | /cloud-audits-often-dont-mean-what-you-think-they-do-230269 | [45] John Scott",5 Essential Characteristics of Cloud Computing Really ", | http://www. inforisktoday.in/5-essential-characteristics-cloud-computing-a-4189. | [46] Jaikumar Vijayan,"Cloud computing 2014 Moving to a zero-trust security | Model - Computerworld3" http://cloudbuzz.com/news/cloud-computing-2014- | Moving -to-a-zero-trust-security-model-computerworld-3/ | [47]" CSA Security, Trust & Assurance Registry (STAR) Cloud Security Alliance | "https://cloudsecurityalliance.org/star/. | [48] "ENISA new steps for building trust in the Cloud — ENISA" . | https://www.enisa.europa.eu/media/news-items/enisa-takes-a-step-forward-in- | building-trust-in-the-cloud. | [49] Mary Scaklett, "How far are we from 'In Cloud We Trust ' – TechRepublic ", | http://www.techrepublic.com/blog/the-enterprise-cloud/how-far-are-we-from-in- | cloud-we-trust/. | [50] From transparency to trust in the Cloud EU Cyber security Agency ENISA | Advises how to implement incident reporting in cloud computing — ENISA Press. | release jan 2014 http://www.enisa.europa.eu/media/press-releases | /from-transparency-to-trust-in-the-cloud-eu-cyber-security -agency-enisa-advises-how-to-implement- | incident-reporting-in-cloud-computing. | [51]Linda Mushthaler" Is your trust in cloud services misplaced or | true Find out with a cloud trust rating - Network World" , | Feb 2014 http://www.networkworld.com/newsletters/techexec/ | 2014/022114-cloud-trust-ratings.html. | [52] Fariborz Farahmand ,"Risk Perception and Trust in Cloud", | http://www.isaca.org/Journal/Past-Issues/2010/Volume-4/Pages/Risk-Perception-and-Trust-in-Cloud.aspx | [54] "RSA Consumer Identity Protection - Cloud Storage – EMC" | http://www.emc.com/emc-plus/rsa-thought-leadership/cloud/index | [55] Anthony Plewes "Security and the cloud building trust Orange | Business Services anothony plewes march 2014 " http://www.orange-business.com/en | /blogs/connecting-technology/cloud-computing/security-and-the- | cloud-building-trust. | [56]Alan Joch, "Should you trust disaster recovery to the cloud -- | FCW",http://fcw.com/articles/2012/10/26/disaster-recovery-cloud | .aspx. | [57] Neelie Kroes ,"Standards for the Cloud - European Commission | 2013 "http://ec.europa.eu/commission_2010-2014/kroes/en/content | standards-cloud.html. | [58] "What is CloudAudit - Definition from WhatIs.com" | http://searchcloudsecurity.techtarget.com/definition/CloudAudit.html | [60] Kara Daeyermenjian Your cloud computing SLA can't be a mark | eting gimmick http://searchcloudprovider.techtarget.com/feature/ | Your-cloud-computing-SLA-cant-be-a-marketing-gimmick. | [61] ,Coco Cloud project in the news In the press: 28/03/2014 | http://ec.europa.eu/digital-agenda/en/news/coco-cloud-project-news | [62] Kristian Steenstrup, Gartner The Internet of Things is moving | the mainstream , February 7, 2014. | [63] Dr. Selva Selvaratnam Top secure identity trends for2014 information Week http://www.informationweek.in/informationweek/news-analysis/287317/secure-identity-trends-2014?utm_source=rss&utm_medium=rss&utm_campaign=top-secure-identity-trends-for-2014 | [64]NIST definition of cloud computing,US department of Commerce | http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. | | |